UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/598,631	06/21/2000	Robert Daniel Maher III	NR-2	6324

7590 03/10/2005	**EXAMINER**
Craig J cOX	LEMMA, SAMSON B
Netrake Corporation	

ART UNIT	PAPER NUMBER
2132	

Craig J cOX
Netrake Corporation
3000 Technology Drive
Suite 100
Plano, TX 75074

DATE MAILED: 03/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	**Applicant(s)**
Office Action Summary	09/598,631	MAHER ET AL.
	Examiner	**Art Unit**	
	Samson B Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _21 June 2000_.

2a) ☒ This action is **FINAL.**   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-16_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-16_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All   b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   This office action is in replay to an amendment filed on October 04, 2004. Claims 1-16

are pending.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art
> are such that the subject matter as a whole would have been obvious at the time the invention was made to a
> person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

3.   **Claims 1- 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth

(U.S. Patent No. 6,598,034) in view of Lorrain et al (hereinafter referred as Lorrain)(U.S. Patent

No. 6,636,512).

4.   **As per claim 1**, Kloth discloses a method for preventing denial of service attacks over a

data

network including a plurality of traffic flows each formed by a plurality of data

packet, the method comprising:

       scanning the contents of the data packet; (column 4, lines 40-43)

       verifying that the data packets conform to a set of predetermd

       requirements; (column 4, lines 40-45; column 6, lines 18-20; column 5, lines 4-10]

       checking if the data packet is associated with a validated traffic flow; and [column 10,

lines 38-46; column 10, lines 55-57]

kloth discloses that a rule (requirement) generator for providing rules for processing the

data packets according to the analyzed bit patterns; and the rules are applied to the bit

patterns which are parsed from the IP flow and IP packets traffic types and priorities resulting

form application of the rules (requirements) are mapped onto the existing Quality of service

(QOS) assignments.(column 16, lines 43-49). Kloth further discloses the different service level

can be used to further decide the appropriate routing speed (priority) to be applied to the data

packet.(column 7, lines 45-49].

Kloth does not explicitly teach placing the data packet in a higher priority quality of service if

the data

packet is associated with a validate traffic flow; and to a low priority quality of service if it is

not associated with a validate traffic flow. However, Lorrain discloses reserving bandwidth for

higher priority quality of service if the data packet is associated with a Real Time (RT] traffic

(interpreted as "validated traffic" by the office) and serving the packet that is associated with

Non Real Time (NRT) traffic (interpreted by the office as "non validated traffic") with lower

quality of service, after the all higher priority traffic has been served.(column 2, lines 20-37].

 Accordingly, It would have been obvious to one having ordinary skill in the art at the invention

was made to combine the Kloth's assignment of different Quality of service as per teachings of

Lorrain's in order to prevent denial of service by placing the data packet in a higher priority

quality of service if the data packet is associated with a Real Time or validated traffic flow and

to a low priority quality of service if it is not associated with a Real Time traffic flow (validated

traffic flow).

5.   **As Claim 7**, Kloth discloses the method of preventing denial of service attacks on a data

network

which includes a plurality of traffic flows each formed by multiple data packets

having header and payload information, the method using a network device

comprising a traffic flow scanning engine; and a quality of service processor having

a low priority queue and higher priority queues, the method comprising:

    scanning the header information using traffic flow scanning engine; (column 4, lines 40-

    43; column 3, lines 62-63)

    reordering and reassembling the data packets using the traffic flow scanning

    engine; [column 7, lines 26-28]

    flagging data packets that do not reorder or reassemble correctly to be

    dropped; [column 12, lines 5-11]

    scanning the payload contents using the traffic flow scanning engine; [column 8, lines

    37-47; column 3, lines 62-63; column 10, lines 38-42]

    determining whether the data packets conform to a set of predetermined

    requirements; [column 4, lines 40-45; column 6, lines 18-20; column 5, lines 4-10]

    flagging data packets that do not conform to be dropped; [column 5, lines 4-10]

    checking if the data packets are associated with a validated traffic flow; and [column

    10, lines 38-46; column 10, lines 55-57]

kloth discloses that a rule (requirement) generator for providing rules for processing the data

packets according to the analyzed bit patterns; and the rules are applied to the bit patterns

which are parsed from the IP flow and IP packets traffic types and priorities resulting form

application of the rules (requirements) are mapped onto the existing Quality of service (QOS)

assignments.(column 16, lines 43-49). Kloth further discloses the different service level can be

used to further decide the appropriate routing speed (priority) to be applied to the data

packet.(column 7, lines 45-49].

Kloth does not explicitly teach assigning the data packets to a higher priority quality of service

if the data

packet is associated with a validate traffic flow; and to a low priority quality of service if the

data packet is not associated with a validate traffic flow. Kloth does not also explicitly teach

flagging the data packets that do not reorder or reassemble correctly to be dropped and

flagging data packets that do not conform to be dropped.

However, Lorrain discloses reserving bandwidth for higher priority quality of service if the data

packet is associated with a Real Time (RT] traffic (validated traffic) and serving the packet that

is associated with Non Real Time (NRT) traffic or non validated traffic with lower quality of

service, after the all higher priority traffic has been served.(column 2, lines 20-37].

Lorrain further discloses that packets that are dropped with in the network are flagged as

discardable packets through the use of so- called Discardable Eligibility (DE) identifier bit.[

column 2, lines 17-19]

 Accordingly, It would have been obvious to one having ordinary skill in the art at the invention

was made to combine the Kloth's assignment of different Quality of service and at the same

time flagging of the dropped packets as per teachings of Lorrain's in order to prevent denial of

service by assigning the data packet in a higher priority quality of service if the data packet is

associated with a Real Time or validated traffic flow and to a low priority quality of service if it

is not associated with a Real Time traffic flow (validated traffic flow) and drop packets that do

not satisfy the requirements.

6.   **As per claim 12,** Kloth discloses a network device for preventing denial of service

attacks on a data

network which includes a plurality of traffic flows each formed by multiple data

packets having contents including header information and payload information, the

network device comprising:

        a traffic flow scanning engine operable to scan the header and payload

information of the data packets, to associate each data packet with a particular

traffic flow and to determine whether each traffic flow is a validated traffic flow or

a non-validated traffic flow, wherein the traffic flow scanning engine is further

operable to reorder and reassemble the data packets and to verify that the data

packet conforms to predetermined requirements such that the traffic flow scanning engine

produces a conclusion associated with each data packet; and (column 4, lines 40-43; column

3, lines 62-63; column 3,

column 8, lines 37-46; column 3, lines 62-63; column 7, lines 30-49; column 7, lines 26-28;

column 4, lines 40-45; column 6, lines 18-20; column 5, lines 4-10; column 4, lines 12-13].

Kloth discloses a quality of service processor connected to the traffic flow scanning engine

and operable to place the data packets into a quality of service queue from a

plurality of quality of service queues based on the conclusion from the traffic flow

scanning engine,(column 7, lines 41-45; column 12, lines 60-67, figure 11]

kloth discloses that a rule (requirement) generator for providing rules for processing the data

packets according to the analyzed bit patterns; and the rules are applied to the bit patterns

which are parsed from the IP flow and IP packets traffic types and priorities resulting form

application of the rules (requirements) are mapped onto the existing Quality of service (QOS)

assignments.(column 16, lines 43-49). Kloth further discloses the different service level can be

used to further decide the appropriate routing speed (priority) to be applied to the data

packet.(column 45-49].

Kloth does not explicitly teaches a quality of service processor connected to the traffic flow

scanning engine

and operable to place the data packets into a quality of service queue from a

plurality of quality of service queues based on the conclusion from the traffic flow

scanning engine, wherein data packet from non-validated traffic flows are assigned

to a low priority queue and data packets form validated traffic flow are assigned to a

higher priority queue based on its contents. However, Lorrain discloses reserving bandwidth for

higher priority quality of service if the data packet is associated with a Real Time (RT] traffic

(validated traffic) and serving the packet that is associated with Non Real Time (NRT) traffic or

non validated traffic with lower quality of service, after the all higher priority traffic has been

served.(column 2, lines 20-37].

Accordingly, It would have been obvious to one having ordinary skill in the art at the invention

was made to combine the Kloth's assignment of different Quality of service as per teachings of

Lorrain's in order to prevent denial of service by assigning the data to a low priority quality

queue for the data packet if it is not associated with a Real Time traffic flow (validated traffic

flow) and assigned to higher priority queues based on its content.

7.   **As per claim 2,** the combination of Kloth and Lorrain teach the method as applied to

claim 1 above. Furthermore Kloth teaches the method wherein verifying includes insuring that

the

data packet reorder and reassemble according to a defined policy and insuring that the

data packets conform to required parameters. (column 7, lines 26-28; column 6, lines 32-35;

column 5, lines 4-10).

8.   **As per claim 3,** the combination of Kloth and Lorrain teach the method as applied to

claim 1 above. Furthermore Kloth teaches the method further comprising between verifying

and

checking:

> dropping the data packet if it does not conform to the set of predetermined
>
> requirements. (column 5, lines 4-10)

9.   **As per claim 4,** the combination of Kloth and Lorrain teach the method as applied to

claim 3 above. Furthermore Kloth teaches the method wherein scanning includes scanning of

the

data packet's header information and scanning of the data packet's payload contents.(column

8, lines 40-42]

10.   **As per claim 5, 8 and 16** the combination of Kloth and Lorrain teach the method as

applied to claim 1, 7 and 12 above. Furthermore Kloth teaches the method wherein the

predetermined requirements

include packet length, non-overlapping offset fields, and adherence to protocol

standards. (column 4,lines 5-8]

11.   **As per claim 6 and 11,** the combination Kloth and Lorrain teach the method as applied

to claim 5 and 7 above. Furthermore Lorrain teaches the method wherein the validated traffic

flows are

identified by a state associated with each traffic flow.(column 2, lines 20-37;column 12, lines

17-19]

12.   **As per claim 9,** the combination Kloth and Lorrain teach the method as applied to

claim 7 above. Furthermore Lorrain teaches the method wherein flagged data packets are

dropped by

the traffic flow scanning engine. (column 2, lines 15-19]

13.   **As per claim 10,** the combination Kloth and Lorrain teach the method as applied to

claim 7 above. Furthermore Lorrain teaches the method wherein flagged data packets are

dropped by

the quality of service processor [column 2, lines 15-19]

14.   **As per claim 13,** the combination Kloth and Lorrain teach the method as applied to

claim 12 above. Furthermore Lorrain teaches the method wherein the low priority queue is

assigned to a maximum percentage of network bandwidth. (column 2, lines 31-36)

15.   **As per claim 14**, the combination Kloth and Lorrain teach the method as applied to claim

12 above. Furthermore Kloth teaches the method wherein traffic packets that do not reorder or

reassemble correctly and data packets that do not conform to the predetermined requirements

are dropped by the network device.[column 12, lines 5-10]

16.   **As per claim 15,** the combination Kloth and Lorrain teach the method as applied to

claim 12 above. Furthermore Lorrain teaches the method wherein the traffic flows are

identified by a state associated with each traffic flow, the state representing whether the

traffic flow is validated or non-validated.[column 2, lines 20-37].(It is interpreted by the office

that Real Time traffic are considered to be a validated traffice and on the hand Non Real Time

Traffic are considered to be Non-Validated traffic).

Response to Arguments

17.   Applicant's argument filed on October 10, 2004 have been fully considered but they are

not persuasive.

Applicants first argued that both the references used in rejections of the claims

namely **Kloth** and **Lorrain** discloses network systems for examining traffic and providing

quality of service however the invention, on the other hand, is designed to prevent denial of

service attacks which can disrupt network services. In response to applicant's arguments, the

recitation "A method for preventing denial of service attacks" has not been given patentable

weight because the recitation occurs in the preamble. A preamble is generally not accorded

any patentable weight where it merely recites the purpose of a process or the intended use of a

structure, and where the body of the claim does not depend on the preamble for completeness

but, instead, the process steps or structural limitations are able to stand alone. See *In re

Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88

USPQ 478, 481 (CCPA 1951). Furthermore, according to Newton's Telecom Dictionary, 19th

Edition, March 2003, CMP Books, where Prevention of denial of service is defined: "the

prevention of Denial of Service attacks requires five key components 1, Upgrade **2. Use a

firewall**. Firewalls can help prevent attacks by blocking unauthorized users. **3. Intrusion

detection**. Intrusion detection help monitor the network and detect the sign of different

attacks. **4. Virus protection,** Denial of service attacks are often propagated by worms, virus

and Trojan horses that plant small programs on the system. and 5. Diligence." **Kloth**, the

primary reference on the record, discloses that the invention can provide (among others) the

following capabilities : **Firewall, Intruder detection, virus detection**, and backdoor intrusion

protection.[Column 5, lines 13-15] and [Column 10, lines 43-45]. Furthermore, **Kloth** discloses

that packets associated with a certain source address might also be dropped or discarded, if it

has been determined that the source address is sending undesirable materials. [Column 5,

lines 8-10]. Therefore, the primary reference in the record, namely **Kloth** implicitly discloses

the "Method of preventing denial of service attacks" for the reasons explained above,

accordingly, the examiner respectfully disagrees with the first argument by the applicant.

The second argument by the applicant is traversing the Examiners reading of "real time traffic" in Lorrain with the concept of "validated traffic" and "Non-real time traffic" in Lorrain with the concept of "non-validated traffic" as used by the applicants. Applicants argued that validated traffic is independent of the type of traffic, i.e. validated traffic can be real time or non-real time traffic. **In response to this second argument,** for the sake of argument, let us assume that a validated traffic can be real time or non-real time just as the applicant suggested. The major elements of the applicants claim is setting/placing the data packet in a higher priority of service if the data packet is associated with a validated traffic flow; and to a low priority quality of service if it is not associated with a validated traffic.[See for instance applicants 1st claim].This implies that the applicant will set both the real time traffic and non-real time traffic higher priority. Indeed, one of ordinary skill would not have been motivated to set the same high priority to both real-time traffic and non-real time traffic, since this does not only increase congestion but it is contrary to the practice of optimizing and utilization of the bandwidth/resources. [See Lorrain column 2, lines 20-38] and this is contrary to the method of preventing denial of service attacks, since denial of service attacks is characterized by consuming resources.

Lastly, applicants argued the following that neither Kloth, nor Lorrain, individually or in combination, describe validating traffic flows, as claimed in Claims 1-16 of the present application. As described with reference to Figure 5, validating traffic flows include examining the flow to insure that it conforms to expected characteristics such as reordering or reassembling correctly, and conforming to enforced protocols, and by insuring that the flow itself is validated by checking flow parameters over enough data packets for it to be classified. Also, validating a particular flow is inherently different than determining if traffic is real time or non-real time. Determining real time from non-real time traffic requires only examining the header of the packet to determine the protocol, such as RTP, UDP, or TCP, which indicates the type of traffic in the packet. Validating as described above requires knowledge in the network

equipment of the characteristics of the particular protocols to check to see if the packets conform to those protocols, as well as knowledge of the **source of the packets** such as **matching** physical input information against **source address/port information** in the header, and even knowledge of attributes of the customer associated with the **source address**. None of the types of validating, as set out by the Applicant, is described by Kloth or Lorrain who merely look at **header information** to determine the type of traffic.

Examiner disagrees with the above applicant last argument.

Examiner would point out that **Kloth** does not merely look at the header information to determine the type of traffic. Rather, **Kloth** discloses all parts of the IP flow all, for instance the IP header, TCP header, Application header, is analyzed by the routing engine. The routing engine will receive and parse an incoming IP flow. For the outset, the engine looks at (or analyzes) all parts of the IP flow, for instance the IP header, TCP header, Application header, etc. A set of rules are used to define a pattern (or set of patterns) to be analyzed (or compared/matched) in the incoming IP data flow. [Column 4, lines 39-61]. Kloth further indicate that present invention provides for looking at every part of a packet, with the packet being part of an IP flow coming into the routing engine. [Column 10, lines 17-19]. In yet another aspect, **Kloth** discloses that the routing assignments are mapped onto existing Quality of Service (QoS) and/or Class of Service (CoS) capabilities.[Column 4, lines 62-64] . Furthermore **Kloth** discloses that it should be further noted that in parsing the entire IP flow, a virus or the like might be detected in the payload (or other bits) of the IP flow. Relevant infected packets or bit patterns might thereafter be discarded, and/or corrected. [Column 10, lines 39-42]. Accordingly, the present system performs the route lookup in parallel to the lookup of the rest of the attributes of the particular packet, i.e. both lookups are done in parallel. [Column 4, lines 5-8]. Accordingly, applicants second argument of merely looking at header information is not valid for the reasons explained above.

Likewise Examiner disagrees to the fact that **Kloth** does not considers the **source/address** when validating the flow. In response to this applicant argument, Examiner would point out Kloth on column 5, lines 4-10 stating the following. "In still another aspect, the data flow (or packets) might be dropped intermittently, or discarded altogether, as a result of a detected data pattern. For instance, all data packets associated with a certain virus pattern might be dropped or discarded. Packets associated with a **certain source address** might also be dropped or discarded, if it has been determined that **that source address is sending** undesired materials. [Column 5, lines 4-10]. Furthermore, **Kloth** indicates that traffic flow from "spammers" might also be eliminated by detecting the **source address pattern of machines** sending such undesired information, and thereafter dropping any packets from that source address.[Column 10, lines 43-46]

Therefore every elements of the limitation of the claim explicitly or implicitly suggested and disclosed by the combinations of the references in the record and the rejection remains valid.

Conclusion

18.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
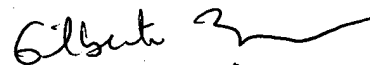
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
SL
03/02/2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100